ПОИСК ЭФФЕКТИВОГО РЕШЕНИЯ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОТ КИБЕРУГРОЗ СООБЩЕСТВА МИКРОСЕТЕЙ СО ВЗАИМОСВЯЗАННЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Гурина Л.А.[1], Айзенберг Н.И.[2]

Цель исследования: *разработка методического подхода для обеспечения кибербезопасности взаимосвязанных микросетей в составе энергетического сообщества.*

Методы исследования: *вероятностные методы, кооперативная и некооперативная теория игр.*

Результат исследования: *Проведен анализ возможных угроз и уязвимостей информационно-коммуникационной инфраструктуры сообщества микросетей. Предложена модель коалиций микросетей, учитывающая такие факторы, как риски кибербезопасности, располагаемые ресурсы микросетей для защиты от кибератак и возможные последствия реализованных киберугроз. Разработана методика определения эффективности защиты от киберугроз в составе коалиций и без для сообщества микросетей. Предусматривается учёт синергетических эффектов при обеспечении кибербезопасности энергетического сообщества в случае объединения в коалиции отдельных микросетей через определение положительного и отрицательного взаимовлияния защищенности и киберугроз исследуемых объектов друг на друга. Для оценки эффективности объединения предложен метод определения совместного выигрыша коалиции, а также справедливое перераспределение дополнительного выигрыша между участниками. Приводятся результаты оценивания эффективности возможного объединения в коалиции для сообщества микросетей на основе вектора Шепли.*

Научная новизна *состоит в том, что для оценки эффективности возможного объединения в коалиции микросетей с целью обеспечения кибербезопасности энергетического сообщества в работе предложен теоретико-игровой подход, сочетающий в себе приемы оценки рисков кибербезопасности на основе теорий вероятностей и нечетких множеств и приемы кооперативной теории игр, предлагающей способы справедливого дележа вложений для организации мер по защите от кибератак.*

Ключевые слова: *энергетическое сообщество, риски кибербезопасности, кибератаки, коалиции, кооперативная игра.*

DOI:10.21681/2311-3456-2023-3-37-49

Введение

Благодаря поставленным целям по декарбонизации и развитию технологий силовой электроники, массовая интеграция микросетей на основе возобновляемых источников энергии (ВИЭ) в электрические сети стала мировой тенденцией в последнее десятилетие [1, 2]. Все более активно прослеживается тенденция масштабного перехода на индивидуальное энергоснабжение на основе распределенной генерации с выработкой энергии за счет использования ВИЭ [3]. Развитие распределенной генерации на основе возобновляемых и гибридных источников энергии в энергетических системах, а также участие активных потребителей в выработке энергии, требует для нормального функционирования такой энергосистемой интеллектуальных методов управления и мониторинга с использованием различных информационных и коммуникационных технологий.

Вместе с тем применение интеллектуальных счетчиков электроэнергии, цифровых измерительных устройств и оборудования на основе различного аппа-

1 Гурина Людмила Александровна, кандидат технических наук, доцент, старший научный сотрудник Лаборатории управления функционированием электроэнергетических систем Института систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, Россия. E-mail: gurina@isem.irk.ru

2 Айзенберг Наталья Ильинична, кандидат экономических наук, доцент, старший научный сотрудник Лаборатории реформирования электроэнергетики Института систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, Россия. E-mail: zen@isem.irk.ru

ратного и программного обеспечения трансформирует энергетические системы в сложные киберфизические энергетические системы (КФЭС) с критической информационной инфраструктурой [4, 5]. Отличительной особенностью КФЭС является сильное взаимодействие между ее подсистемами, что влечет за собой новые вызовы и угрозы, которые необходимо учитывать при управлении ими [6, 7]. К таким вызовам и угрозам можно отнести цифровизацию объектов энергетики, обусловливающих возникновение рисков кибербезопасности [8] при функционировании энергетических сообществ. Распределенные источники энергии используются для реализации преимуществ местного производства возобновляемой энергии, а интеллектуальные счетчики все чаще устанавливаются на объектах потребителей для облегчения управления спросом. Микросеть — это локализованная группа источников электроэнергии и нескольких нагрузок, которые могут быть подключены к традиционной энергосистеме или могут работать изолированно [9]. Эти распределенные объекты могут взаимодействовать с центром управления или между собой через многочисленные каналы связи, что повышает вероятность кибератак и непреднамеренных ошибок [10]. Отказы аппаратного и программного обеспечения компонента микросети могут повлиять на всю информационно-коммуникационную инфраструктуру сообщества, в первую очередь из-за подключения их к общей сети, что усиливает последствия кибератак для функционирования микросетей [11, 12].

Энергетическое сообщество технически представляет собой группу микросетей или объектов (например, взаимосвязанные нагрузки и распределенные энергоисточники) в четко определенных электрических границах, которые действуют как единый управляемый объект по отношению к внешней электрической сети [13, 14]. Для поддержания приемлемой функциональности управления микросетями и надежного их функционирования важно обеспечение кибербезопасности как информационых систем микросетей, так и информационно-коммуникационной инфраструктуры сообщества микросетей с учетом множества потенциальных угроз и сложной взаимосвязанной структуры. Это требует оценки возможных угроз, выявления уязвимостей и разработки стратегий смягчения последствий кибератак. Разработка мер для сохранения свойств кибербезопасности сообщества микросетей, несмотря на возможное возникновение киберинцидентов, является актуальной задачей.

Учитывая сложность проблемы и лежащие в ее основе сетевые системы, нельзя ожидать успеха от схемы управления без учёта возможного взаимодействия, взаимовлияния отдельных объектов друг на друга. Основой для этого взаимодействия может стать разработка совместной концепции обеспечения кибербезопасности группы микросетей, определения эффективности создания коалиций, в том числе, полагаясь на экономические критерии. Здесь инструментом принятия решений могут быть модели, построенные на платформе теории игр.

Работ, посвященных принятию решений о стратегиях защиты для несотрудничающих друг с другом объектов достаточно много [9, 11, 12]. В то же время, важным видится исследование разработки модели противодействия киберугрозам совместными усилиями группы объектов или микросетей. Критерием оценки эффективности таких моделей может стать не только совместное (учитывающие синергию) снижение последствий кибератак для общей сети (системы), но и экономическая эффективность: когда построенная модель реализует устойчивое Парето оптимальное решение через перераспределение совместных выигрышей. Последнее в работе будет реализовано с привлечением подходов кооперативной теории игр [15].

Основной вклад статьи заключается в разработке методического подхода обеспечения кибербезопасности энергетических сообществ с учетом таких факторов, как риски кибербезопасности, взаимовлияние располагаемых ресурсов микросетей для защиты от кибератак, взаимовлияние последствий киберугроз. Для этой цели разработана модель, основанная на кооперативной теории игр, в соответствии с которой объекты могут образовывать коалиции с учетом получаемых выгод от этого сотрудничества. Используя предложенную модель, проанализированы возможные возникающие коалиционные структуры, а также условия, необходимые для сотрудничества.

Анализ киберугроз информационно-коммуникационной инфраструктуры при управлении сообществом микросетей

При управлении микросетями в составе сообществ используются информационные и коммуникационные технологии в процессе производства, передачи и потребления энергии. Соответственно, операции микросетей интегрируют технологический процесс с функциями управления, вычислений, связи и, реализуемыми информационно-коммуникационной инфраструктурой сообщества. Информационно-коммуни-

кационная инфраструктура сообщества микросетей состоит из центра управления, множества датчиков и исполнительных механизмов, встроенных в полевые устройства. Обмен информацией между микросетями позволяет найти оптимальную стратегию для эффективной и надежной работы сообщества. Для управления сообществом микросетей существуют различные структуры управления, которые могут иметь централизованную, децентрализованную, распределенную и иерархическую архитектуру. На рис. 1 представлен пример сообщества со взаимосвязанными информационными и технологическими инфраструктурами микросетей.

Преимуществами межсетевого объединения микросетей в сообщества являются:

— совместное использование резервов в критических условиях для снижения вероятности сбоя системы, минимизации требований к аварийному сбросу нагрузки и повышения общей надежности системы,
— экономичная диспетчеризация сообщества микросетей как в режиме подключения к основной сети, так и в изолированном режиме.
— смягчение последствий экстремальных событий и т.д.

Наряду со многими преимуществами, предоставляемыми сообществами, могут возникнуть различные проблемы и сложности, связанные с вопросами кибербезопасности при управлении ими.

В последние годы многие электроэнергетические компании уже модернизировали и улучшили работу своих распределительных сетей, используя технологии интеллектуальных сетей, такие как система управления энергопотреблением (EMS), DMS, автоматизация подстанций (SA) и системы AMI (Advanced Metering Infrastructure) [16-18], которая предоставляет электроэнергетическим компаниям систему двусторонней связи от центра управления до счетчика, а также возможность изменять различные параметры уровня обслуживания клиентов [19]. Расширение технологий AMI и развитие интеллектуальных счетчиков с помощью программ интеллектуальных измерений предоставляют распределительным сетям возможность фиксировать обратную связь по напряжению в точках подключения.

Центр управления микросетями включает в себя сервера приложений, архиватор и человеко-машинного интерфейса (HMI). Сервер приложений оснащен системой диспетчерского управления и сбора данных (SCADA) и EMS. Система SCADA действует как внешний интерфейс для взаимодействия с полевыми устройствами (RTU), тогда как EMS является внутренним процессором с возможностями принятия решений [20].

Система SCADA информационно-коммуникацион-

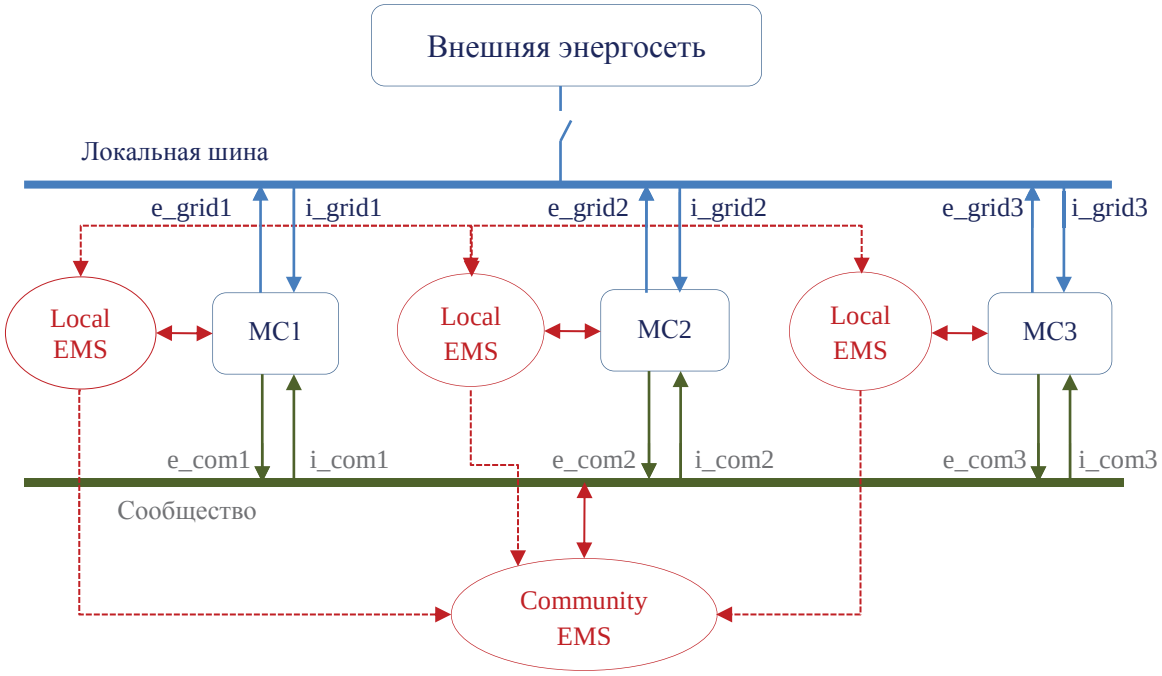

Рис. 1. Структура сообщества микросетей и управления ими

ной инфраструктуры микросетей осуществляет сбор, передачу и обработку информации о функционировании микросетей. Данные отображаются в виде информации о мониторинге и измерений, команд управления, а также конфигураций микросети (например, схема сети, протокол связи, настройки устройства). Система SCADA получает измерения в режиме реального времени и выдает команды диспетчерского управления на полевые устройства. Основываясь на измерениях в реальном времени, собранных системой SCADA, приложение EMS выполняет набор функций для обеспечения безопасности, надежности, экономичности, устойчивости и эффективности функционирования микросетей.

Датчики и исполнительные механизмы внутри полевых устройств представляют собой интерфейсы между информационно-коммуникационной инфраструктурой и компонентами технологической части КФЭС. Датчики устанавливаются для мониторинга и измерения физических процессов в режиме реального времени, что способствует улучшению ситуационной осведомленности для управления микросетями и своевременному обнаружению неисправностей или отказов силового оборудования. Датчики охватывают различные типы измерительных приборов, такие как устройства синхронизированных векторных измерений (PMU) WAMS, RTU системы SCADA и интеллектуальные счетчики (IEC) AMIS (AMI - это интегрированная система интеллектуальных счетчиков, систем управления данными и сетей связи, которые обеспечивают двустороннюю связь между коммунальными службами и потребителями).

Коммуникационная сеть может представлять собой разнородное объединение проводных систем, таких как оптоволокно и кабели, и беспроводных сред, таких как микроволновые и инфракрасные технологии. В дополнение к связи с локальными полевыми устройствами центр управления обычно подключается к внешним источникам информации, включая Интернет и другие центры управления.

Внешние источники обмена информацией для микросетей в составе ЭСо включают устройства, подключенные к Интернету вещей (IoT) (интеллектуальные устройства, которые обеспечивают доступ к данным/управлению через Интернет), сигналы регулирования частоты и т.д. Чем больше добавляется возможностей по приему и обработке различного рода информации из внешних источников, тем более уязвимо сообщество к киберугрозам. Это связано с тем, что интеллектуальные счетчики и другие передовые коммуникационные технологии становятся уязвимыми для атак, если уязвимые части, такие как интерфейсы управления, каналы передачи данных и удаленные порты отладки, не защищены должным образом. Устройства IoT, подключенные к общедоступной сети и сети электрических систем одновременно, могут быть и каналами, через которые могут быть выполнены кибератаки [21, 22]. Благодаря быстрому развитию телекоммуникационных систем IoT может взаимодействовать с беспроводными сенсорными сетями (WSN), радиочастотной идентификацией (RFID), микросетями в любой форме. Возникновение рисков кибербезопасности - это неизбежная проблема, которую необходимо решать при применении IoT. Если проблема не решается должным образом, злоумышленники воспользуются дефектами и уязвимостями устройств или объектов, а затем могут нарушить целостность, доступность и конфиденциальность данных, используемых при управлении микросетями и, тем самым, нарушить их функционирование через глобальную сеть IoT.

Сообщество микросетей может быть уязвимо для следующих угроз кибербезопасности:

- Угрозы, влияющие на качество информационных потоков при управлении микросетями.
- Угрозы, влияющие на системное оборудование и подключенные устройства.
- Угрозы, влияющие коммуникационную сеть.

Для эффективного управления микросетями необходимы потоки данных SCADA, WAMS, AMIS требуемого качества [23]. С позиций кибербезопасности информационные потоки, используемые при управлении должны удовлетворять следующим требованиям:

- Доступность относится к гарантии того, что данные доступны и своевременны. Доступностью данных характеризуется полнотой и требует, чтобы данные измерений были без потерь и своевременными, т.е. доставленными с допустимыми задержками для быстрой адаптации к изменяющимся условиям в критических обстоятельствах.
- Целостность означает обеспечение достоверности данных. Достоверность требует точности и синхронизации по времени измерений в пределах допустимых ошибок без нарушения последовательности поступления данных. При оценке точности необходим учет такого фактора, как согласованность измерений. Достоверность данных должны сохраняться на протяжении всего их жизненного цикла, включая сбор датчиками, передачу по каналам связи, анализ

на серверах приложений, визуализацию HMI и хранение в архиве. При этом данные всегда должны представлять актуальную информацию при любых условиях эксплуатации.

— Конфиденциальность относится к защите данных от доступа. Неожиданное раскрытие конфиденциальной информации может привести к разрушительным последствиям для функционирования микросетей и поведения потребителей.

Наиболее распространенными кибератаками, влияющих на качество измерительной информации, являются атаки внедрения ложных данных (FDI – False Data Injection), DoS-атаки (DoS – Denial of Service) и вредоносное программное обеспечение [24]. Из-за того, что данные чувствительны ко времени, любая задержка, потеря данных или синхронизации данных, а также их искажение (нарушение целостности и доступности) могут затруднить ситуационную осведомленность и повлиять на функционирование сообщества микросетей. При успешных кибератаках на локальную сеть управления, злоумышленниками могут быть сформированы ложные команды по отключению генераторов микросетей. При доступе к интеллектуальным электронным устройствам (IED) злоумышленник может получить информацию о конфигурации сообщества микросети, коммуникационной сети, схеме IED.

Мерами повышения кибербезопасности микросетей могут быть следующие:

— экранирование;

— программные решения кибербезопасности в автоматизированных системах микросетей (антивирус, обнаружение кибератак, программное обеспечение брандмауэра, кодирование и т.д.);

— аппаратные средства автоматизированных систем микросетей (брандмауэры, маршрутизаторы, коммутаторы, шлюзы для защиты сети от нелегального обмена данными и т.д.);

— выбор оптимального маршрута связи [25].

Для обеспечения кибербезопасности микросетей необходимо наличие ресурсов для каждой микросети. При взаимодействии микросетей важно минимизировать влияние ошибок и сбоев в результате кибератак на информационную систему одной микросети на функциональность информационных систем остальных микросетей. Для сохранения свойств кибербезопасности сообщества микросетей предлагается микросети объединять в коалиции. Анализ возможных коалиций методами теории игр позволит найти решение по перераспределению совокупного выигрыша и эффективному использованию ресурсов для защиты сообщества микросетей.

Модель коалиций микросетей

Некооперативная игра

В этом разделе обсудим разработку мер по кибербезопастности в рамках некооперативного и кооперативного подхода. Рассмотрим взвешенный ориентированный граф $G\left(N,\mathfrak{N}^+,\mathfrak{N}^-\right)$, где N — количество узлов. Каждый узел представляет собой микросеть. Объекты, являющиеся «соседями», имеют возможность взаимовлияния в той или иной степени [26]. Множество узлов j, влияющих на узел i обозначено через $\mathfrak{N}_i$. Положительное воздействие узла iна узел j задается с помощью $\varphi_{ij}^b \in (0,1)$, $b \in \{+,-\}$, который показывает силу связи между указанными узлами. Веса взаимовлияния формируют матрицы $\boldsymbol{W}^+$ и $\boldsymbol{W}^-$ с элементами

$$W_{ij}^+ = \begin{cases} 1, & i = j; \\ \varphi_{ij}^+, & j \in \mathfrak{N}_i^+; \\ 0, & i \neq j, j \notin \mathfrak{N}_i, \end{cases} \quad (1)$$

$$W_{ij}^- = \begin{cases} 1, & i = j; \\ \varphi_{ij}^-, & j \in \mathfrak{N}_i^-; \\ 0, & i \neq j, j \notin \mathfrak{N}_i, \end{cases} \quad (2)$$

Каждый объект (микросеть) iN имеет некоторые ресурсы, состоящие из располагаемых технических средств, бюджета и т.д.. Эти ресурсы обеспечивают определенный уровень кибербезовпасности $x_i > 0$, $\boldsymbol{X} = \left(x_1,\ldots,x_n\right)$, который может положительно повлиять на безопасность соседних объектов.

Каждый объект $i \in N$ находится под угрозой d_i, $\boldsymbol{D} = \left(d_1,\ldots,d_n\right)$, которая может негативно повлиять на безопасность соседних объектов. Для любой микросети $i \in N$ со своими собственными угрозами и эффективной защитой необходимо определить получаемую полезность, связанную с $\boldsymbol{X}$ и $\boldsymbol{D}$. На основе вероятности (1) и (2) она определиться как

$$V_{\{i\}}\left(\boldsymbol{W},\boldsymbol{X},\boldsymbol{D}\right) = \pi\left(\left(\left(\boldsymbol{W}^+\right)^T \cdot \boldsymbol{X}\right)_i\right) - c\left(\left(\left(\boldsymbol{W}^-\right)^T \cdot \boldsymbol{D}\right)_i\right). \quad (3)$$

Функции $\pi(\cdot)$ представляют собой прибыль от реализации защиты на основе располагаемого уровня кибербезопасности $\boldsymbol{X}$, $c(\cdot)$ – функция возможных последствий (ущербов) кибератак в каждой микросети

$i \in N$. Каждый объект стремиться максимизировать собственную полезность (эффект) от выбранной стратегии защиты. Такая функция называется характеристической. Можем сформулировать задачу по определению стратегии защиты в форме некооперативной игры (N,V) [27] с имеющими характеристическими функциями полезности микросетей (3): игра независимых объектов, где каждый участник стремиться максимизировать собственную полезность, выбирая уровень вложения ресурсов и степень защиты от киберугроз.

Кооперативная игра

Для возможного улучшения своих кибербезопасности и снижения киберугроз микросети участники могут сотрудничать, формируя коалиции $S \subseteq N$. Пусть коалиционная структура из M коалиций $S = (S_1,\ldots,S_M) \subseteq N$, где $S_k \cap S_l = \varnothing$ при $k \neq l$, $\cup_{\forall k} S_k = N$. Взаимовлияние при объединении в коалицию изменяются и теперь описываются скорректированными матрицами:

$$\bar{W}_{ij}^{+} = \begin{cases} 1, & i = j; \\ W_{ij}^{+}, & i,j \notin S; \\ f^{+}\left(W_{ij}^{+}\right), & i,j \in S, \end{cases} \tag{4}$$

$$\bar{W}_{ij}^{-} = \begin{cases} 1, & i = j; \\ W_{ij}^{-}, & i,j \notin S; \\ f^{-}\left(W_{ij}^{-}\right), & i,j \in S. \end{cases} \tag{5}$$

У рассматриваемых объектов появляется возможность усилить положительное влияние друг на друга, т. е., например, увеличить веса $W_{ij}^{+} \geq 0, \ \forall i,j \in S$, организуя защиту вместе. Даже если два объекта не имеют влияния друг на друга без сотрудничества, т. е. $W_{ij}^{+} \geq 0$, то в коалиции они могут получить дополнительный выигрыш, например, засчёт синергетического эффекта использования совместного бюджета. Второй стороной может стать уменьшение негативного влияния угроз в целом на систему и друг на друга, т.е. снижения $W_{ij}^{-} \geq 0, \ \forall i,j \in S$ за счет обмена информацией и совместного устранения уязвимостей.

При наличии коалиционной структуры можем определить характеристическую функция полезности для коалиции $S \subseteq N$ на основе (4) и (5):

$$V_S\left(\bar{\boldsymbol{W}},\boldsymbol{X},\boldsymbol{D}\right) = \pi\left(\left(\left(\bar{\boldsymbol{W}}^{+}\right)^{T} \cdot \boldsymbol{X}\right)_S\right) - c\left(\left(\left(\bar{\boldsymbol{W}}^{-}\right)^{T} \cdot \boldsymbol{D}\right)_S\right). \tag{6}$$

При этом должны быть выполнены следующие соотношения.

Суммарные совместные положительный эффект от располагаемого уровня кибербезопасности в кооперативной игре должен быть больше или равен суммарному выигрышу микросетей в некооперативной игре

$$\left(\left(\bar{\boldsymbol{W}}^{+}\right)^{T} \cdot \bar{\boldsymbol{X}}\right)_S \geq \sum\nolimits_{\{i\} \in S} \left(\left(\boldsymbol{W}^{+}\right)^{T} \cdot \boldsymbol{X}\right)_i. \tag{7}$$

Суммарные совместные угрозы и уязвимости в кооперативной игре должны быть меньше или равны суммарным угрозам и уязвимостям микросетей в некооперативной игре.

$$\left(\left(\bar{\boldsymbol{W}}^{-}\right)^{T} \cdot \boldsymbol{D}\right)_S \leq \sum\nolimits_{\{i\} \in S} \left(\left(\boldsymbol{W}^{-}\right)^{T} \cdot \boldsymbol{D}\right)_i. \tag{8}$$

Для простоты анализа можно предполагать, что как функции выгоды (эффект) от уровня кибербезопасности $\pi(\cdot)$ и функции затрат на организацию защиты от киберугроз $c(\cdot)$ линейны с коэффициентами наклона α и β соотвественно, тогда

$$V_S\left(\bar{\boldsymbol{W}},\boldsymbol{X},\boldsymbol{D}\right) = \alpha\left(\left(\bar{\boldsymbol{W}}^{+}\right)^{T} \cdot \boldsymbol{X}\right)_S - \beta\left(\left(\bar{\boldsymbol{W}}^{-}\right)^{T} \cdot \boldsymbol{D}\right)_S. \tag{9}$$

Задача может быть смоделирована как (N,S,V) – кооперативная игра в характеристической форме [15, 27] с коалициями S, являющимися разбиениями максимальной коалиции *N* и имеющими характеристическую функцию выигрыша (9): требуется максимизировать полезность коалиции, выбирая уровень кибербезопасности, например, через вложения дополнительных ресурсов, и степень защиты от киберугроз. Описанная задача является теоретико-игровой, сложной. В этой работе рассматриваются вопросы формирования матриц взаимовлияния и определение величины выигрыша в кооперативной игре относительно некооперативного случая для содружества микросетей при неизменных имеющихся у объектов уровнях киберзащиты $\boldsymbol{X}$. Основной вопрос, на который отвечает предложенная модель, как сформировать механизм распределения дополнительного общего выигрыша, который будет интересен всем участникам (объектам) в сравнении с ситуацией некооперативной игры.

Необходимо определить условия реализуемости кооперации, устойчивости максимальной коалиции, а также «справедливом» распределении выигрыша $V(N)$ между игроками. Для того, чтобы существовало решение для определенного разбиения на коалиции

в кооперативной игре необходимо, чтобы выполнялся ряд свойств [15]. В частности, потребуем, чтобы игра была

а) супераддитивной. Это гарантируется выполнением свойств (7), (8);

б) существенной:

$$V_S\left(\bar{W},X,D\right)\geq\sum_{\{i\}\in S}V_{\{i\}}\left(W,X,D\right). \quad (10)$$

В этом случае можно гарантировать существование решения – распределения общего выигрыша коалиции между ее участниками, которое будет Парето улучшать выигрыш каждого игрока коалиции относительно независимых действий по обеспечению защиты от киберугроз вне кооперации. Одним из возможных решений существенной, супераддитивной игры является распределение выигрыша в соответствии с вектором Шепли. Решение по вектору Шепли следует принципу утилитаризма и распределения выигрыша по труду.

Для рассматриваемого случая $V_S\left(\bar{W},X,D\right)$, $S\subseteq N$ вектор Шепли $\omega\left(V\right)$ распределяет выигрыш в коалиции следующим образом:

$$\omega_i\left(V\right)=\sum_{K\subseteq S}\frac{(k-1)!(s-k)!}{n!}\left(V_K\left(\bar{W},X\ D\right)-\right.$$
$$\left.-V_{K-1}\left(\bar{W},X,D\right)\right),i\in S,k=|K|, \quad (11)$$

где $V_{K-1}\left(\cdot\right)$ – значение выигрыша коалиции K без участника $\{i\}$.

Таблица 1

Уровни взаимного влияния уровней кибербезопасности микросетей

Уровень/ диапазон изменения	**Описание**
Низкий $L,[0,0.24]$	Опасность возникновения отказов и сбоев в энергетическом сообществе высокая в результате кибератак на микросеть. Сочетание отказов компонентов и/или ошибок функциональности информационно-коммуникационной инфраструктуры может привести к значительным нарушениям функционирования сообщества микросетей.
Средний $M,[0.25,0.74]$	В результате кибератаки на микросеть возможны незначительные сбои и ошибки в управлении сообществом микросетей, которые устранимы и не оказывают критического влияния на функциональность информационно-коммуникационной инфраструктуры. Реализация функций оперативного управления осуществляется в требуемом объеме и не приводит к нарушениям функционирования сообщества микросетей.
Высокий $H,[0.75,1]$	Влияние кибератак на микросеть не приводит к отказам и сбоям компонентов информационно-коммуникационной инфраструктуры остальных микросетей. Срабатывают все меры по обеспечению кибербезопасности.

Таблица 2

Уровни взаимного влияния последствий кибератаки

Уровень/ диапазон изменения	**Описание**
Низкий $L,[0,0.24]$	Последствия кибератаки на одну из микросетей может иметь незначительное или ограниченное неблагоприятное воздействие на другие и имеет локальный характер.
Средний $M,[0.25,0.74]$	Последствия кибератаки на одну из микросетей может оказать серьезное неблагоприятное воздействие на другие микросети.
Высокий $H,[0.75,1]$	Последствия кибератаки на одну из микросетей может оказать серьезное или катастрофическое неблагоприятное последствие для остальных микросетей.

Методика определения эффективного решения по защите микросетей от киберугроз на основе подходов кооперативной теории игр

Этапы предлагаемой методики следующие:

1. Определение вероятности реализации угрозы на микросеть (вектор $\boldsymbol{D}$).

2. Определение вектора показателей кибербезопасности информационно-коммуникационной инфраструктуры [28] каждой микросети (вектор $\boldsymbol{X}$) согласно следующему алгоритму:

2.1. Оценка риска кибербезопасности $\tilde{R}_i^{Risk}$ каждой микросети при управлении сообществом.

2.2. Оценка кибербезопасности каждой микросети при управлении сообществом определяется как $\tilde{R}_i^{CS} = 1 - \tilde{R}_i^{Risk}$.

Для вектора $\boldsymbol{X}$: $\tilde{R}_i^{CS} = x_i$.

3. Определение матрицы $\boldsymbol{W}^+$ взаимного влияния уровней кибербезопасности микросетей (1). Семантическое описание коэффициентов W_{ij}^+ взаимного влияния уровней кибербезопасности микросетей представлено в табл. 1.

4. Определение матрицы взаимного влияния последствий W^- успешно реализованной кибератаки в сообществе микросетей (2). Семантическое описание коэффициентов взаимного влияния последствий W^- реализованной кибератаки представлено в табл. 2.

5. Определение коэффициентов $f^+\left(W_{ij}^+\right)$ матрицы взаимовлияний уровней кибербезопасности микросети в составе возможных коалиций $\overline{Wij}^+$ согласно выражению:

$$f^+\left(W_{ij}^+\right) = W_{ij}^+ + W_{ji}^+ - W_{ij}^+ \cdot W_{ji}^+, \qquad (12)$$

где W_{ij}^+ – коэффициент матрицы взаимного влияния уровней кибербезопасности микросетей W^+ (1).

6. Определение коэффициентов $f^-\left(W_{ij}^-\right)$ матрицы взаимовлияния киберугроз $\overline{W}^-$. В соответствии с (8) получаем, $f^-\left(W_{ij}^-\right) \le W_{ij}^-$. В случае «идеальной» кооперации участникам удается полностью устранить негативные последствия взаимовлияния угроз между членами коалиции. Если это сделать невозможно, то взаимовлияние внутри коалиции снижается до минимума относительно некооперативного случая.

$$f^-\left(W_{ij}^-\right) = \min\left\{W_{ij}^-, W_{ji}^-\right\}, \qquad \forall i, j \in S. \qquad (13)$$

Для реализации предложенной методики разработан алгоритм поиска наиболее эффективной защиты от кибератак информационно-коммуникационной инфраструктуры микросетей на основе кооперативной теории игр:

1. Определение вектора вероятностей реализации угроз D на микросети

2. Определение уровня кибербезопасности X для отдельных игроков.

3. Определение матрицы положительного взаимного влияния W_{ij}^+ (1) в зависимости от уровня кибербезопасности микросетей (табл. 1).

4. Определение матрицы взаимного влияния W_{ij}^- (2) последствий кибератак на микросети (табл. 2).

5. Формирование матриц $\overline{W}_{ij}^+$ и $\overline{W}_{ij}^-$ взаимовлияния в случае кооперации для разных коалиций в соответствии с (4), (5), (12) и (13).

6. Определение эффектов обеспечения кибербезопасности в рамках некооперативной $V_{\{i\}}\left(W, X, D\right)$ и кооперативной $V_S\left(\overline{W}, X, D\right)$ игр для разных коалиций в соответствии с (3) и (9).

7. Проверка условия супераддитивности (7), (8) и существенности игры (10).

8. Определение эффективного для каждого участника перераспределения выигрыша от создания киберзащиты при объединении в коалицию для каждой микросети через вектор Шепли (11) в случае кооперативной игры.

Пример

Для поиска наиболее эффективного объединения микросетей в коалицию с целью защиты от кибератак и сохранения приемлемого уровня кибербезопасности рассмотрим сообщество микросетей со взаимосвязанными информационными системами (рис. 1). Количество микросетей, входящих в состав сообщества равно трем. Определим две ситуации: каждая микросеть действует отдельно или в составе коалиции.

Условно зададим вектор вероятностей реализации угрозы на микросети сообщества $\boldsymbol{D} = (0,53; 0,67; 0,41)$ и вектор уровней кибербезопасности микросетей $\boldsymbol{X} = (0,75; 0,71; 0,82)$.

Пусть матрица взаимного положительного влияния имеющегося уровня кибербезопасности микросетей для некооперативной игры

$$W_{ij}^+ = \begin{matrix} 1 & 0,47 & 0,33, \\ 0,4 & 1 & 0,27 \\ 0,2 & 0,1 & 1 \end{matrix}$$

а матрица взаимного влияния последствий успешно реализованной кибератаки в сообществе микросетей

$$W_{ij}^- = \begin{matrix} 1 & 0,27 & 0,52. \\ 0,59 & 1 & 0,41 \\ 0,6 & 0,5 & 1 \end{matrix}$$

Рассмотрим возможные коалиции и условия взаимодействия в них. Имеем следующие варианты: {1,2} и {3}; {1,3} и {2}; {2,3} и {1}; {1,2,3}.

Для представленных коалиций необходимо рассчитать матрицы взаимовлияний $\bar{W}^+$ и $\bar{W}^-$ по формулам (4) и (5). В соответствии с пунктом 5 и 6 методики, формулами (13) и (14), при вступлении в коалицию определяем коэффициенты $f^+\left(W_{ij}^+\right), f^-\left(W_{ij}^-\right)\ i,j \in S$. В нашем случае для $f^-\left(W_{ij}^-\right)$ мы выбираем точный минимум взаимовлияния (14).

Ниже приведены найденные матрицы взаимовлияния $\bar{W}_{ij}^+$ и $\bar{W}_{ij}^-$ для коалиции {1,3} и {2}:

$$\bar{W}_{ij}^+ = \begin{matrix} 1 & 0,47 & 0,46 \\ 0,4 & 1 & 0,27 \\ 0,46 & 0,1 & 1 \end{matrix}$$

$$\bar{W}_{ij}^- = \begin{matrix} 1 & 0,37 & 0,52 \\ 0,59 & 1 & 0,41 \\ 0,52 & 0,5 & 1 \end{matrix}$$

и {1,2,3}:

$$\bar{W}_{ij}^+ = \begin{matrix} 1 & 0,68 & 0,46 \\ 0,68 & 1 & 0,34 \\ 0,46 & 0,34 & 1 \end{matrix}$$

$$\bar{W}_{ij}^- = \begin{matrix} 1 & 0,37 & 0,52 \\ 0,37 & 1 & 0,41 \\ 0,52 & 0,41 & 1 \end{matrix}$$

Для остальных случаев объединения микросетей в коалицию матрицы взаимовлияния $\bar{W}_{ij}^+$ и $\bar{W}_{ij}^-$ определяются аналогично.

Эффективность защиты для каждой микросети в некооперативном случае рассчитывается в соответствии с (3), с применением линейной интерпретации функции выигрыша (9), где $\alpha = 1$ и $\beta = 1$ определены в некоторых условных единицах. Результаты расчёта эффективности защиты представлены в табл. 3. Первая строка соответствует эффективности защиты от кибератак (3), которые имеет каждая микросеть, без вступления в коалицию.

Можно проверить, что для изначально заданных и вновь сформированных матриц взаимовлияния, а также векторов $\boldsymbol{X}$ и $\boldsymbol{D}$ выполняется условия (7) и (8). Условия существенности игры (10) можно проверить после расчета выигрышей на основе (9) для всех уровней коалиций. Результаты представлены в табл. 3. Совместные выигрыши в составе коалиций выделены жирным.

Наибольший выигрыш имеет коалиция, куда входят все участники или максимальная коалиция {1,2,3}. Возможно перераспределение полученного выигрыша, рассчитанное на основе вклада каждого участника для обеспечения кибербезопасности. Оно существует, так как выполняются условия (7), (8) и (10). Одним из вариантов может стать распределение по вектору Шепли для максимальной коалиции {1,2,3}. Например, микросеть 1 получит следующую долю совокупного выигрыша:

$$\omega_1(V) = \frac{1}{3}\cdot V\left(\{1\}\right) + \frac{1!}{3!}\cdot\left(V\left(\{1,2\}\right) - V\left(\{2\}\right)\right) +$$

$$+\frac{1}{6}\cdot\left(V\left(\{1,3\}\right) - V\left(\{3\}\right)\right) + \frac{1}{3}\cdot\left(V\left(\{1,2,3\}\right) -$$

$$-V\left(\{2,3\}\right)\right) = 0,38,$$

а весь вектор Шепли будет равен ω = **(0, 38; 0, 35; 0, 28)** в долях относительно общего выигрыша, равного 1,54. В последней строке табл. 3 представлены получаемые выигрыши в условных бюджетных единицах внутри коалиции, определенные по вектору Шепли. Можно видеть, что любая микросеть получит выигрыш больший в составе максимальной коалиции,

Таблица 3

Выигрыши микросетей V_S в составе различных коалиций, в условных единицах

Коалиции/микросеть	**1**	**2**	**3**	**Сумма**
{1},{2},{3}	0,03	0,07	0,30	0,40
{1,2},{3}	**0,61**		0,30	0,91
{1,3},{2}	**0,68**	0,07	----	0,75
{2,3},{1}	0,03	**0,66**		0,69
{1,2,3}	**1,54**			1,54
Дележ по Шепли в {1,2,3}	0,58	0,54	0,43	1,54

чем, если бы она в коалицию не вступала (первая и последняя строка табл.3). Среди малых коалиций наиболее эффективной представляется коалиция {1,2}, но она будет неустойчивой, так как от присоединения микросети 3 все участники выигрывают.

Таким образом, показано, что объединение микросетей в коалиции позволяет эффективнее использовать имеющиеся ресурсы для обеспечения кибербезопасности.

Выводы

Проведен анализ возможных угроз и уязвимостей информационно-коммуникационной инфраструктуры сообщества микросетей. Показано, что для обеспечения кибербезопасности взаимосвязанных информационных систем в зависимости от имеющихся ресурсов защиты микросетей целесообразно объединять их в коалиции. Разработана модель оценки эффективности коалиции микросетей, на основе которой предложен методический теоретико-игровой подход определения решения по защите от кибератак. Развитие работы предполагает разработку оптимизационного блока модели, определяющего эффективное перераспределение ресурсов для организации защиты сообщества микросетей, обеспечивающих необходимый уровень кибербезопасности.

Работа выполнена в рамках научного проекта «Теоретические основы, модели и методы управления развитием и функционированием интеллектуальных электроэнергетических систем», № FWEU-2021-0001.

Литература

1. E. Papadis and G. Tsatsaronis. Challenges in the decarbonization of the energy sector. Energy. 2020, vol. 205, 118025. DOI:10.1016/j.energy.2020.118025.
2. M. Erdiwansyah and H Husin, et al. A critical review of the integration of renewable energy sources with various technologies. Protection and Control of Modern Power Systems. 2021, vol. 6, no. 3. DOI: 10.1186/s41601-021-00181-3.
3. G. V. B. Kumar, R. K. Sarojini, K. Palanisamy, S. Padmanaban, and J. B. Holm-Nielsen. Large scale renewable energy integration: Issues and solutions. Energies. 2019, vol. 12, no. 10, 1996. DOI: 10.3390/en12101996.
4. N. Voropai. Electric power system transformations: A review of main prospects and challenges. Energies. 2020, vol. 13, no. 21, 5639. DOI: 10.3390/en13215639.
5. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. In IEEE Access. 2020, vol. 8, pp. 151019-151064. DOI: 10.1109/ACCESS.2020.3016826.
6. X. Cai, Q. Wang, Y. Tang and L. Zhu. Review of Cyber-attacks and Defense Research on Cyber Physical Power System. 2019 IEEE Sustainable Power and Energy Conference (iSPEC), Beijing, China. 2019, pp. 487-492. DOI: 10.1109/iSPEC48194.2019.8975131.
7. I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access. 2021, vol. 9, pp. 29775–29818. DOI: 10.1109/ACCESS.2021.3058403.
8. L. Gurina, T. Zoryna, and N. Tomin. Risk assessment for digitalization of facilities of cyber-physical energy system. 2022 International Ural Conference on Electrical Power Engineering (UralCon), Magnitogorsk, Russian Federation. 2022, pp. 86–90. DOI: 10.1109/UralCon54942.2022.9906686.
9. E. Hossain, E. Kabalcı, R. Bayindir, and R Perez. A comprehensive study on microgrid technology. International Journal of Renewable Energy Research. 2014, vol. 4, pp. 1094–1104.
10. J. L. Gallardo, M. A. Ahmed and N. Jara. LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid. In IEEE Access. 2021, vol. 9, pp. 124295-124312. DOI: 10.1109/ACCESS.2021.3110873.
11. C. Wang, T. Zhang, F. Luo, F. Li, and Y. Liu. Impacts of cyber system on microgrid operational reliability. IEEE Transactions on Smart Grid. 2019, vol. 10, no. 1, pp. 105–115. DOI: 10.1109/TSG.2017.2732484.
12. A. D. Frias, N. Yodo and O. P. Yadav. Mixed-Degradation Profiles Assessment of Critical Components in Cyber-Physical Systems. 2019 Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL, USA. 2019, pp. 1-6. DOI: 10.1109/RAMS.2019.8769014.
13. Gjorgievski V.Z., Cundeva S., Georghiou G.E.. Social arrangements, technical designs and impacts of energy communities: A review. Renewable Energy. 2021, vol. 169, pp. 1138-1156. DOI: 10.1016/j.renene.2021.01.078.
14. Warneryd M., Håkansson M., Karltorp K. Unpacking the complexity of community microgrids: A review of institutions' roles for development of microgrids. Renewable and Sustainable Energy Reviews. 2020, 121, 109690, DOI: 10.1016/j.rser.2019.109690.
15. Parilina E., Reddy P.V., and Zaccour. Cooperative Games. In Theory and Applications of Dynamic Games: A Course on Noncooperative and Cooperative Games Played over Event Trees. Cham: Springer International Publishing. 2022, pp. 39-63. DOI: 10.1007/978-3-031-16455-2_2.
16. S. Rathor and D Saxena. Energy management system for smart grid: An overview and key issues. International Journal of Energy Research. 2020. DOI:10.1002/er.4883.
17. I. Rendroyoko, A. D. Setiawan and Suhardi. Development of Meter Data Management System Based-on Event-Driven Streaming Architecture for IoT-based AMI Implementation. 2021 3rd International Conference on High Voltage Engineering and Power Systems (ICHVEPS), Bandung, Indonesia. 2021, pp. 403-407. DOI: 10.1109/ICHVEPS53178.2021.9601104.

18. X. Liang, F. Liang, B. Zhou, H. Pan and L. Yuan. Key Technologies Research and Equipment Development of Smart Substation Automation System. 2020 IEEE Sustainable Power and Energy Conference (iSPEC), Chengdu, China. 2020, pp. 1736-1741. DOI: 10.1109/iSPEC50848.2020.9351156.
19. A. N. Milioudis and G. T. Andreou. Use of Smart Metering Data for Distribution Network Operational Status Assessment. 2021 IEEE Madrid PowerTech, Madrid, Spain. 2021, pp. 1-6. DOI: 10.1109/PowerTech46648.2021.9494894.
20. S. Li, B. Jiang, X. Wang, and L. Dong. Research and application of SCADA system for the microgrid. Technologies. 2017, vol. 5, no. 2, 12. DOI: 10.3390/technologies5020012.
21. S. Mishra, K. Anderson, B. Miller, K. Boyer, and A. Warren. Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. Applied Energy. 2020, vol. 264, 114726. DOI: 10.1016/j.apenergy.2020.114726.
22. Y. Lu and L. D. Xu. Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal. April 2019, vol. 6, no. 2, pp. 2103–2115. DOI: 10.1109/JIOT.2018.2869847.
23. Колосок И.Н., Гурина Л.А. Оценка качества данных SCADA и WAMS при кибератаках на информационно-коммуникационную инфраструктуру ЭЭС // Информационные и математические технологии в науке и управлении. 2020, 1(17), с. 68-78. DOI: 10.38028/ESI.2020.17.1.005.
24. Колосок И.Н., Гурина Л.А. Оценка показателей киберустойчивости систем сбора и обработки информации в ЭЭС на основе полумарковских моделей // Вопросы кибербезопасности. 2021, №6(46), с. 2-11. DOI: 10.21681/2311-3456-2021-6-2-11.
25. Fardad Noorollah, Soleymani Soodabeh, Faghihi Faramarz. Cyber defense analysis of smart grid including renewable energy resources based on coalitional game theory. Journal of Intelligent & Fuzzy Systems. 2018, vol. 35(2), pp. 2063–2077. DOI: 10.3233/JIFS-171980.
26. Iqbal A., Gunn L. J., Guo M., Babar M. A., & Abbott D. Game theoretical modelling of network/cybersecurity. In IEEE Access. 2019, vol. 7, pp. 154167-154179. DOI: 10.1109/ACCESS.2019.294835.
27. Laraki Rida, Jérôme Renault, and Sylvain Sorin. Mathematical foundations of game theory. New York, NY, USA: Springer, 2019. DOI: 10.1007/978-3-030-26646-2.
28. Гурина Л.А. Оценка киберустойчивости системы оперативно-диспетчерского управления ЭЭС // Вопросы кибербезопасности. 2022, №3 (49), с. 23-31. DOI: 10.21681/2311-3456-2022-3-23-31.

SEARCH FOR AN EFFECTIVE SOLUTION TO PROTECT MICROGRID COMMUNITY WITH INTERCONNECTED INFORMATION SYSTEMS AGAINST CYBER THREATS

Gurina L.A.[3], Aizenberg N.I.[4]

The research aims *to develop a methodological approach to ensure the cybersecurity of interconnected microgrids within the energy community.*

The research relies *on the probabilistic methods, cooperative and non-cooperative game theory.*

Research result: *Potential threats and vulnerabilities of the information and communication infrastructure of the microgrids community are analyzed. A proposed model of microgrids coalitions take into account such factors as cybersecurity risks, the available microgrids resources to protect against cyber-attacks, and the consequences of implemented cyber threats. The developed method determines the effectiveness of protection against cyber threats with and without coalitions for the microgrids community. It is planned to take into account synergistic effects in ensuring the cybersecurity of the energy community for the coalition of microgrids by determining the positive and negative mutual influence of the security and cyber threats of the objects on each other. To evaluate*

3 Liudmila A. Gurina, Ph.D. in engineering, Associate Professor, Senior Researcher in the Laboratory for Control of Electric Power Systems at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E-mail: gurina@isem.irk.ru

4 Natalia I. Aizenberg, Ph.D. in economic, Associate Professor, Senior Researcher in the Laboratory of Electric Power Industry Restructuring at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E-mail: zen@isem.irk.ru

the effectiveness of the coalition in the work, we proposed a method for determining the joint gain of the coalition and a fair redistribution of the additional gain between the participants. The result of evaluating the effectiveness of a possible coalition for the microgrids community is based on the Shapley vector.

***The scientific novelty** lies in the fact that in order to evaluate the effectiveness of a possible coalition of microgrids in order to ensure the cybersecurity of the energy community, we use a game-theoretic approach that combines techniques for evaluating cybersecurity risks based on theories of probability and fuzzy sets and techniques of cooperative game theory, which offers ways a fair division of investments to organize measures to protect against cyber attacks.*

***Keywords:** energy community, cybersecurity risk, cyber-attacks, coalitions, cooperative game.*

References

1. E. Papadis and G. Tsatsaronis. Challenges in the decarbonization of the energy sector. Energy. 2020, vol. 205, 118025. DOI:10.1016/j.energy.2020.118025.
2. M. Erdiwansyah and H Husin, et al. A critical review of the integration of renewable energy sources with various technologies. Protection and Control of Modern Power Systems. 2021, vol. 6, no. 3. DOI: 10.1186/s41601-021-00181-3.
3. G. V. B. Kumar, R. K. Sarojini, K. Palanisamy, S. Padmanaban, and J. B. Holm-Nielsen. Large scale renewable energy integration: Issues and solutions. Energies. 2019, vol. 12, no. 10, 1996. DOI: 10.3390/en12101996.
4. N. Voropai. Electric power system transformations: A review of main prospects and challenges. Energies. 2020, vol. 13, no. 21, 5639. DOI: 10.3390/en13215639.
5. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. In IEEE Access. 2020, vol. 8, pp. 151019-151064. DOI: 10.1109/ACCESS.2020.3016826.
6. X. Cai, Q. Wang, Y. Tang and L. Zhu. Review of Cyber-attacks and Defense Research on Cyber Physical Power System. 2019 IEEE Sustainable Power and Energy Conference (iSPEC), Beijing, China. 2019, pp. 487-492. DOI: 10.1109/iSPEC48194.2019.8975131.
7. I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access. 2021, vol. 9, pp. 29775–29818. DOI: 10.1109/ACCESS.2021.3058403.
8. L. Gurina, T. Zoryna, and N. Tomin. Risk assessment for digitalization of facilities of cyber-physical energy system. 2022 International Ural Conference on Electrical Power Engineering (UralCon), Magnitogorsk, Russian Federation. 2022, pp. 86–90. DOI: 10.1109/UralCon54942.2022.9906686.
9. E. Hossain, E. Kabalcı, R. Bayindir, and R Perez. A comprehensive study on microgrid technology. International Journal of Renewable Energy Research. 2014, vol. 4, pp. 1094–1104.
10. J. L. Gallardo, M. A. Ahmed and N. Jara. LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid. In IEEE Access. 2021, vol. 9, pp. 124295-124312. DOI: 10.1109/ACCESS.2021.3110873.
11. C. Wang, T. Zhang, F. Luo, F. Li, and Y. Liu. Impacts of cyber system on microgrid operational reliability. IEEE Transactions on Smart Grid. 2019, vol. 10, no. 1, pp. 105–115. DOI: 10.1109/TSG.2017.2732484.
12. A. D. Frias, N. Yodo and O. P. Yadav. Mixed-Degradation Profiles Assessment of Critical Components in Cyber-Physical Systems. 2019 Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL, USA. 2019, pp. 1-6. DOI: 10.1109/RAMS.2019.8769014.
13. Gjorgievski V.Z., Cundeva S., Georghiou G.E.. Social arrangements, technical designs and impacts of energy communities: A review. Renewable Energy. 2021, vol. 169, pp. 1138-1156. DOI: 10.1016/j.renene.2021.01.078.
14. Warneryd M., Håkansson M., Karltorp K. Unpacking the complexity of community microgrids: A review of institutions' roles for development of microgrids. Renewable and Sustainable Energy Reviews. 2020, 121, 109690, DOI: 10.1016/j.rser.2019.109690.
15. Parilina E., Reddy P.V., and Zaccour. Cooperative Games. In Theory and Applications of Dynamic Games: A Course on Noncooperative and Cooperative Games Played over Event Trees. Cham: Springer International Publishing. 2022, pp. 39-63. DOI: 10.1007/978-3-031-16455-2_2.
16. S. Rathor and D Saxena. Energy management system for smart grid: An overview and key issues. International Journal of Energy Research. 2020. DOI:10.1002/er.4883.
17. I. Rendroyoko, A. D. Setiawan and Suhardi. Development of Meter Data Management System Based-on Event-Driven Streaming Architecture for IoT-based AMI Implementation. 2021 3rd International Conference on High Voltage Engineering and Power Systems (ICHVEPS), Bandung, Indonesia. 2021, pp. 403-407. DOI: 10.1109/ICHVEPS53178.2021.9601104.
18. X. Liang, F. Liang, B. Zhou, H. Pan and L. Yuan. Key Technologies Research and Equipment Development of Smart Substation Automation System. 2020 IEEE Sustainable Power and Energy Conference (iSPEC), Chengdu, China. 2020, pp. 1736-1741. DOI: 10.1109/iSPEC50848.2020.9351156.
19. A. N. Milioudis and G. T. Andreou. Use of Smart Metering Data for Distribution Network Operational Status Assessment. 2021 IEEE Madrid PowerTech, Madrid, Spain. 2021, pp. 1-6. DOI: 10.1109/PowerTech46648.2021.9494894.
20. S. Li, B. Jiang, X. Wang, and L. Dong. Research and application of SCADA system for the microgrid. Technologies. 2017, vol. 5, no. 2, 12. DOI: 10.3390/technologies5020012.
21. S. Mishra, K. Anderson, B. Miller, K. Boyer, and A. Warren. Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. Applied Energy. 2020, vol. 264, 114726. DOI: 10.1016/j.apenergy.2020.114726.

22. Y. Lu and L. D. Xu. Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal. April 2019, vol. 6, no. 2, pp. 2103–2115. DOI: 10.1109/JIOT.2018.2869847.
23. Kolosok I.N., Gurina L.A. Ocenka kachestva dannyh SCADA i WAMS pri kiberatakah na informacionno-kommunikacionnuyu infrastrukturu EES // Informacionnye i matematicheskie tekhnologii v nauke i upravlenii [Information and mathematical tehnologies in science and management], 2020, № 1(17), pp. 68-78. DOI: 10.38028/ESI.2020.17.1.005.
24. Kolosok I.N., Gurina L.A. Otsenka pokazatelei kiberustoichivosti sistem sbora i obrabotki informatsii v EES na osnove polumarkovskikh modelei // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2021, №6. S. 2-11. DOI: 10.21681/2311-3456-2021-6-2-11.
25. Fardad Noorollah, Soleymani Soodabeh, Faghihi Faramarz. Cyber defense analysis of smart grid including renewable energy resources based on coalitional game theory. Journal of Intelligent & Fuzzy Systems. 2018, vol. 35(2), pp. 2063–2077. DOI: 10.3233/JIFS-171980.
26. Iqbal A., Gunn L. J., Guo M., Babar M. A., & Abbott D. Game theoretical modelling of network/cybersecurity. IEEE Access. 2019, vol. 7, pp. 154167-154179. DOI: 10.1109/ACCESS.2019.294835.
27. Laraki Rida, Jérôme Renault, and Sylvain Sorin. Mathematical foundations of game theory. New York, NY, USA: Springer, 2019. DOI: 10.1007/978-3-030-26646-2.
28. Gurina L.A. Ocenka kiberustojchivosti sistemy operativno-dispetcherskogo upravleniya EES // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2022, №3 (49). S. 23-31. DOI: 10.21681/2311-3456-2022-3-23-31.